UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

Richard Allen Sapp,

Plaintiff,

v.

City of Baudette; City of Big Lake; City of Brooklyn Park; City of Buffalo Lake; City of Burnsville; Cass County; City of Golden Valley; Hennepin County; City of Inver Grove Heights; Pipestone County; City of St. Paul; City of Thief River Falls; Washington County; City of White Bear Lake; City of Woodbury; Michael Campion, in his individual capacity as the Commissioner of the Department of Public Safety; Ramona Dohman, in her individual capacity as the Commissioner of the Department of Public Safety; John and Jane Does (1 - 200) acting in their individual capacity as supervisors, officers, deputies, staff, investigators, employees or agents of the other governmental agencies; Department of Public Safety Does (1-30) acting in their individual capacity as officers, supervisors, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety; and Entity Does (1-50) including cities, counties, municipalities, and other entities sited in Minnesota,

Defendants.

Civil File No.

COMPLAINT

JURY TRIAL DEMANDED

For his Complaint, for which Plaintiff demands trial by jury on all claims so triable, Plaintiff Richard Sapp ("Richard") hereby states and alleges as follows:

INTRODUCTION

This is a case to redress the abuse of power by numerous law-enforcement personnel and public employees who illegally accessed the Minnesota Department of Public Safety's system for maintaining the personal, private information of Minnesota citizens. Officers and employees from several different law-enforcement agencies and entities chose to violate federal law, Minnesota and federal policy and the statutorily protected privacy rights of Plaintiff.

These personnel violated the federal Driver's Privacy Protection Act ("DPPA") by unlawfully accessing their protected driver's license information without a purpose permitted under the DPPA. More disturbing, these personnel, charged with protecting and serving the public, knowingly abused their position of trust simply to satisfy their shallow desires to peek behind the curtain into the private lives of Plaintiff, without their knowledge or consent, and without ever informing them of their activities. In fact, they carried on these searches surreptitiously and concealed them from Plaintiff and, presumably, from their supervisors and others. Those charged with oversight of the system, including the Commissioners, concealed this from Plaintiff by failing to ever notify him of these intrusions and violations, and concealed the extent of the violations from the general public. The utter disregard for their privacy rights by law-enforcement personnel, public employees, and others caused Plaintiff emotional distress.

The State of Minnesota, itself, has found that at least 50% of all officers statewide are engaged in the use of this database for purposes not permitted by the DPPA, and therefore violating federal civil and criminal laws. Moreover, the access permitted to

law-enforcement officers, public employees, and others is easily obtained and makes highly private information available, including health information and social security numbers. Plaintiff has no control over the Defendants obtaining his personal information, and impermissible, and inappropriate obtaining has been deliberately concealed and conducted in a surreptitious fashion. These Defendants are the window-peepers of the electronic data age. Through lax policies and apathetic enforcement of the law, these officials and governmental units have caused direct damage to Plaintiff, just as they have trampled upon the clear legislative protections of all citizens' right to feel secure in their privacy.

General Background of Law and Facts

1. This is an action for injunctive relief and money damages for injuries sustained when personnel from various entities in Minnesota illegally obtained Plaintiff's private, personal and confidential driver's license information without a legitimate or permissible law-enforcement purpose or any other lawful purpose.

2. These law-enforcement personnel, public employees, and others viewed and obtained Richard's private information nearly 50 times between 2003 and 2013.

3. Attached to this Complaint as Exhibit A is a copy of an audit prepared by the Minnesota Department of Public Safety showing the obtainments of Plaintiff's wife, Katherine Ann Sapp's ("Katherine") driver's license information by name, not by license plate number, with her driver's license number removed, and showing the "station," meaning the police department, sheriff's office, or other government entity through which the officer obtained her information.

4. Attached to this Complaint as Exhibit B is a copy of an audit prepared by the Minnesota Department of Public Safety showing the obtainments of Richard's driver's license information by name, not by license plate number, with his driver's license number removed, and showing the "station," meaning the police department, sheriff's office, or other government entity through which the officer obtained his information.

5. Without legitimate, permissible reasons, these individuals obtained Plaintiff's private information from Department of Vehicle Services' ("DVS") database.

6. Upon information and belief, these individuals further impermissibly used or disclosed Plaintiff's' private information without a purpose permitted under the DPPA.

7. Each unauthorized, impermissible use, disclosure, or obtainment of their private information, made without a permissible purpose and while acting under color of state and federal law, constituted behavior prohibited by federal statute, and agency and departmental regulations prohibiting some or all of the conduct engaged in by Defendants in this case.

8. Plaintiff bring this action pursuant to 42 U.S.C. § 1988, 28 U.S.C. § 1331, and the Driver's Privacy Protection Act ("DPPA") 18 U.S.C. § 2721 *et seq.*

9. The aforementioned statutory and constitutional provisions confer original jurisdiction of this Court over this matter.

10. The amount in controversy exceeds $75,000, excluding interests and costs.

The Parties

11. Richard Allen Sapp ("Richard") is, and was at all times material herein, a citizen of the United States and a resident of the State of Minnesota.

12. Defendant Cass County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

13. Defendant Hennepin County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

14. Defendant Pipestone County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

15. Defendant Washington County is a county in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

16. Defendant City of Baudette is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

17. Defendant City of Big Lake is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

18. Defendant City of Brooklyn Park is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

19. Defendant City of Buffalo Lake is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

20. Defendant City of Burnsville is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

21. Defendant City of Golden Valley is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

22. Defendant City of Inver Grove Heights is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

23. Defendant City of St. Paul is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

24. Defendant City of Thief River Falls is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

25. Defendant City of White Bear Lake is a home rule charter city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

26. Defendant City of Woodbury is a statutory city in Minnesota, which can be sued under Minn. Stat. § 466.01 *et seq.*

27. Defendants Entity Does (1-50) are various unknown municipalities as defined by Minn. Stat. § 466.01, subd. 1 that can be sued under Minn. Stat. § 466.01 *et seq*. or other statutes, and federal departments and agencies, which can be sued under 28 U.S.C. § 1346 or other statutes.

28. Plaintiff will refer to the entities named in paragraphs 12 to 27 above, along with the Entity Does, collectively as the "Defendant Entities" or "Entity Defendants."

29. Defendants John and Jane Does (1-200), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting in their individual capacities as law-enforcement

supervisors, officers or employees of the Defendant Entities or other federal, state, county or municipal entities in Minnesota.

30. Plaintiff will refer to the individual Defendants (with the exception of the "Commissioner Defendants," "Department of Public Safety Defendants" and "Supervisor Defendants" defined below), including John and Jane Does, collectively as the "Individual Defendants" or "Defendant Individuals."

31. Plaintiff will refer to the Defendants with supervisory authority over the Individual Defendants, including any John and Jane Does with such supervisory authority, collectively as the "Defendant Supervisors" or "Supervisor Defendants."

32. Defendant Michael Campion ("Campion"), upon information and belief, was, at all times material herein, a citizen of the United States and a resident of the State of Minnesota, duly appointed and acting in his individual capacity as the Commissioner of the Minnesota Department of Public Safety.

33. Defendant Mona Dohman ("Dohman"), upon information and belief, was, at all times material herein, a citizen, of the United States and a resident of the State of Minnesota, duly appointed and acting in her individual capacity as the Commissioner of the Minnesota Department of Public Safety.

34. Plaintiff will refer to the Defendants Campion and Dohman collectively, as the "Commissioner Defendants" or "Defendant Commissioners."

35. Defendants DPS Does (1-30), upon information and belief, were, at all times material herein, citizens of the United States and residents of the State of Minnesota, duly appointed and acting their individual capacities as officers, supervisors,

employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety.

36. Plaintiff will refer to officers, supervisors, employees, staff, employees, independent contractors or agents of the Minnesota Department of Public Safety who created, installed, monitored, regulated, coded, enforced, supervised, maintained, oversaw, updated, or otherwise worked on the DVS database or BCA database, each of which contained Plaintiff's private driver's license information (collectively or individually, "DPS Databases" as "Department of Public Safety Does" or "DPS Does.")

FACTUAL ALLEGATIONS

Plaintiff and His Wife are Well-Known in the Law-Enforcement Community as Both Have Worked for Law-Enforcement Agencies and Have Other Family Who Have as Well

37. Richard is married to Katherine.

38. Katherine and Richard have been married since 2001.

39. Richard grew up in North St. Paul.

40. Richard's father was the Chief of Police for North St. Paul.

41. Richard has been a police officer since 1994, working first for the Minnesota State Fair Grounds, and then for Rush City.

42. Since 1999, Richard has been a police officer for the North Branch Police Department.

43. From 1992 to 1997, Richard dated Jennifer Rivard ("Rivard").

44. Richard and Rivard lived together in Roseville from approximately 1995 to 1997.

45. After they broke up in 1997, Richard had no contact with Rivard until a few years later when she called him asking for a couch. Richard did not give Rivard the couch.

46. In the mid-2000's, Richard called the Brooklyn Park Police Department in the course of his police duties for the North Branch Police Department. Richard was surprised that Rivard answered his call. Richard had not known that Rivard worked for the Brooklyn Park Police Department. During that call, they made small talk.

47. Until receiving his audit, Richard did not think about that conversation again. But Katherine's and Richard's audits each reveal that someone, who they believe must be Rivard, started repeatedly (Katherine 14 times and Richard 21 times) obtaining their driver's license information around the time of that call.

48. Katherine has never spoken to, met or even seen a picture of Rivard.

49. Katherine and Richard spoke with a Lieutenant with the Brooklyn Park Police Department about their concerns about Rivard likely repeatedly accessing their drivers' license information.

50. This Lieutenant confirmed that Rivard had been the one who looked up the Sapps so frequently from Brooklyn Park.

51. Because DPS has not identified the individuals who looked up Plaintiff, until he can learn these identities in discovery, Plaintiff will refer to this Brooklyn Park law-enforcement personnel, who he highly suspects is Rivard, as an Individual Jane Doe Defendant.

52. Although they would not be able to identify what car Rivard drives, Richard and Katherine are concerned that Rivard was obtaining their home address through the DPS Database to stalk them.

53. Katherine worked as a 911 dispatcher for Washington County between 1997 and 2001.

54. Katherine's sister is married to a Minneapolis Police officer who joined that Department in 1999.

55. On May 15, 2009, the Minneapolis Star Tribune published an article about Katherine and her siblings.

56. As shown in Exhibit A, the day after that article appeared in the paper, Katherine was looked up by someone from the Minnesota Department of Natural Resources ("DNR").

57. Katherine received a letter in 2013, from the DNR explaining that its employee's access of her driver's license information was not for an official, government related purpose.

58. Katherine is a member of a purported class-action against the aforementioned individual from the DNR.

59. Richard lives in North Branch, Minnesota and has lived there since 1999.

Law Enforcement Officers and Personnel from Entities Across Minnesota Viewed Plaintiff's Private Information Outside the Scope of Any Investigation or Official Police Business

60. The Driver and Vehicle Services Division ("DVS") of the DPS maintains a database containing the motor vehicle records of Minnesota drivers. ("DVS Database").

61. The DVS Database contains "personal information" and "highly restricted personal information," as defined by 18 U.S.C. § 2725 ("Private Data"), including but not limited to names, dates of birth, driver's license numbers, addresses, driver's license photos, weights, heights, social security numbers, various health and disability information, and eye colors of Minnesota drivers, both current and former information dating back to the driver's first license issued in Minnesota.

62. The Minnesota Driver's License Application states: "you must provide your Social Security Number…"

63. According to the Minnesota Driver's License Application, "[i]f you don't provide the information requested, DPS cannot issue you a driver's permit, license, or identification card, and your existing driving privileges, may be affected."

64. As early as 2003, Individual Defendants began looking up Plaintiff's Private Data on the DVS Database without a permissible purpose.

65. After the Individual Defendants looked up Plaintiff's Private Data, they gained knowledge of the contents of the Private Data. In gaining such knowledge, the Individual Defendants obtained Plaintiff's Private Data.

66. Exhibit B, incorporated herein, is an audit provided by DPS showing each time Richard's Private Data was obtained or used by an Individual Defendant.

67. There are several permissible accesses listed in Exhibit B related to accesses made by non-parties, but as to Entity Defendant, all the entries in Exhibit B were not permissible.

68. Exhibit A, incorporated herein, is an audit provided by DPS showing each time Katherine's Private Data was accessed.

69. Each act of the Individual Defendants in obtaining Plaintiff's Private Data also constituted a disclosure by the Commissioner Defendants, because any release or obtainment of information, whether permitted or not, necessarily requires a disclosure; and the method of setting up the DVS Database and of providing constant access to it constituted a disclosure of Private Data under the DPPA.

70. Column "EsupportStationName" of Exhibit A and B, incorporated herein, reflect the department or entity which, upon information and belief, employed the Individual Defendant that obtained or used Plaintiff's Private Data.

71. Column "EsupportPath" of Exhibit A and B, incorporated herein, reflect the type of Private Data that was obtained or used by the Individual Defendant.

72. Columns "AccessDay" and "AccessDate," of Exhibit A and B, incorporated herein, reflect the day of the week, date, and time when the Individual Defendant obtained or used Plaintiff's Private Data.

73. DPS does not provide the name of the individual who obtained or used Plaintiff's Private Data.

74. Each line of Exhibit A and B, incorporated herein, reflects the audit of each time Plaintiff's information, upon information and belief, was obtained or used by an Individual Defendant without a permissible purpose.

75. Officers employed by, licensed by, or otherwise accessing through the City of Baudette obtained Richard's Private Data for purposes not permitted by the DPPA one time.

76. Defendant Baudette's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

77. Richard has never been to the City of Baudette, never been charged with or suspected of committing a crime in the City of Baudette, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Baudette, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Baudette.

78. Rather, Baudette's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Baudette's personnel.

79. Officers employed by, licensed by, or otherwise accessing through the City of Big Lake obtained Richard's Private Data for purposes not permitted by the DPPA one time.

80. Defendant Big Lake's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

81. Richard never been charged with or suspected of committing a crime in the City of Big Lake, has never been involved in any civil, criminal, administrative, or

arbitral proceeding in or involving the City of Big Lake, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Big Lake.

82. Rather, Big Lake's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Big Lake's personnel.

83. Officers employed by, licensed by, or otherwise accessing through the City of Brooklyn Park obtained Richard's Private Data for purposes not permitted by the DPPA twenty-one (21) times.

84. Defendant Brooklyn Park's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

85. Richard has never been charged with or suspected of committing a crime in the City of Brooklyn Park, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Brooklyn Park, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Brooklyn Park.

86. Rather, Brooklyn Park's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Brooklyn Park's personnel.

87. Officers employed by, licensed by, or otherwise accessing through the City of Buffalo Lake obtained Richard's Private Data for purposes not permitted by the DPPA one time.

88. Defendant Buffalo Lake's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

89. Richard has never been to or even heard of the City of Buffalo Lake, never been charged with or suspected of committing a crime in the City of Buffalo Lake, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Buffalo Lake, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Buffalo Lake.

90. Rather, Buffalo Lake's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Buffalo Lake's personnel.

91. Officers employed by, licensed by, or otherwise accessing through the City of Burnsville obtained Richard's Private Data for purposes not permitted by the DPPA one time.

92. Defendant Burnsville's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

93. Richard has never been charged with or suspected of committing a crime in the City of Burnsville, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Burnsville, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Burnsville.

94. Rather, Burnsville's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Burnsville's personnel.

95. Officers employed by, licensed by, or otherwise accessing through Cass County obtained Richard's Private Data for purposes not permitted by the DPPA one time.

96. Defendant Cass County's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

97. Richard went to a training and at Clandestine Lab refresher classes with a number of Cass County deputies.

98. Richard has never been charged with or suspected of committing a crime in Cass County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Cass County, and there was no legitimate reason for Richard to have been the subject of any investigation by Cass County.

99. Rather, Cass County's obtainment and use of Richard's personal information was for purposes that were purely personal to Cass County's personnel.

100. Officers employed by, licensed by, or otherwise accessing through the City of Golden Valley obtained Richard's Private Data for purposes not permitted by the DPPA one time.

101. Defendant Golden Valley's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

102. Richard has never been charged with or suspected of committing a crime in the City of Golden Valley, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Golden Valley, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Golden Valley.

103. Rather, Golden Valley's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Golden Valley's personnel.

104. Officers employed by, licensed by, or otherwise accessing through Hennepin County obtained Richard's Private Data for purposes not permitted by the DPPA two times.

105. Defendant Hennepin County's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

106. Richard has never been charged with or suspected of committing a crime in Hennepin County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Hennepin County, and there was no legitimate reason for Richard to have been the subject of any investigation by Hennepin County.

107. Rather, Hennepin County's obtainment and use of Richard's personal information was for purposes that were purely personal to Hennepin County's personnel.

108. Officers employed by, licensed by, or otherwise accessing through the City of Inver Grove Heights obtained Richard's Private Data for purposes not permitted by the DPPA three times.

109. Defendant Inver Grove Heights' obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

110. Richard has never been charged with or suspected of committing a crime in the City of Inver Grove Heights, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Inver Grove Heights, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Inver Grove Heights.

111. Rather, Inver Grove Heights' obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Inver Grove Heights' personnel.

112. Officers employed by, licensed by, or otherwise accessing through Pipestone County obtained Richard's Private Data for purposes not permitted by the DPPA one time.

113. Defendant Pipestone County's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

114. Richard has never been to Pipestone County, never been charged with or suspected of committing a crime in Pipestone County, has never been involved in any

civil, criminal, administrative, or arbitral proceeding in or involving Pipestone County, and there was no legitimate reason for Richard to have been the subject of any investigation by Pipestone County.

115. Rather, Pipestone County's obtainment and use of Richard's personal information was for purposes that were purely personal to Pipestone County's personnel.

116. Officers employed by, licensed by, or otherwise accessing through the City of St. Paul obtained Richard's Private Data for purposes not permitted by the DPPA three times.

117. Defendant St. Paul's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

118. Richard has never been charged with or suspected of committing a crime in the City of St. Paul, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of St. Paul, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of St. Paul.

119. Rather, St. Paul's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of St. Paul's personnel.

120. Officers employed by, licensed by, or otherwise accessing through the City of Thief River Falls obtained Richard's Private Data for purposes not permitted by the DPPA one time.

121. Defendant Thief River Falls' obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

122. Richard has never been to Thief River Falls, never been charged with or suspected of committing a crime in the City of Thief River Falls, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Thief River Falls, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Thief River Falls.

123. Rather, Thief River Falls' obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Thief River Falls' personnel.

124. Officers employed by, licensed by, or otherwise accessing through Washington County obtained Richard's Private Data for purposes not permitted by the DPPA two times.

125. Defendant Washington County's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

126. Richard has never been charged with or suspected of committing a crime in Washington County, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving Washington County, and there was no legitimate reason for Richard to have been the subject of any investigation by Washington County.

127. Rather, Washington County's obtainment and use of Richard's personal information was for purposes that were purely personal to Washington County's personnel.

128. Officers employed by, licensed by, or otherwise accessing through the City of White Bear Lake obtained Richard's Private Data for purposes not permitted by the DPPA one time.

129. Defendant White Bear Lake's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

130. Richard has never been charged with or suspected of committing a crime in the City of White Bear Lake, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of White Bear Lake, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of White Bear Lake.

131. Rather, White Bear Lake's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of White Bear Lake's personnel.

132. Officers employed by, licensed by, or otherwise accessing through the City of Woodbury obtained Richard's Private Data for purposes not permitted by the DPPA one time.

133. Defendant Woodbury's obtainment and use of Richard's personal information was not for any use in carrying out any law enforcement, governmental, judicial, or litigation-related function.

134. Richard has never been charged with or suspected of committing a crime in the City of Woodbury, has never been involved in any civil, criminal, administrative, or arbitral proceeding in or involving the City of Woodbury, and there was no legitimate reason for Richard to have been the subject of any investigation by the City of Woodbury.

135. Rather, Woodbury's obtainment and use of Richard's personal information was for purposes that were purely personal to the City of Woodbury's personnel.

136. Officers employed by the Entity Defendants, along with those Individual Defendants currently identified as John and Jane Does, obtained or used Richard's Private Data approximately nearly 50 times for reasons not permitted under the DPPA.

137. Each of the above obtainments was committed knowingly; each of the above obtainments was for a reason not permitted under the DPPA, meaning that the Defendants had no law-enforcement reason for obtaining the information.

138. Defendants obtained the information for curiosity, animosity, or other personal reasons completely unrelated to their position as law-enforcement officers, public employees, or in their job functions.

139. Individual Defendants viewed Plaintiff's Private Data from his State-issued driver's licenses including his home address, color photographs or images, date of birth,

eye color, height, weight, driver identification number, and upon information and belief, social security information

140. Curiosity about or animosity toward Plaintiff or other personal reasons are not purposes permitted for obtaining information under the DPPA.

141. The Individual Defendants mentioned above who obtained this information did so using Plaintiff's name, not pursuant to a license plate look-up, and there is seldom any law-enforcement function that would permit accessing Plaintiff's private information by name.

142. Plaintiff was not involved in any criminal activity nor suspected of any such activity.

143. Plaintiff had not committed any act that would entitle Entity Defendants and Individual Defendants to obtain his information under any of the permissible exceptions to the DPPA; to the extent any such permissible reason could exist, Plaintiff has eliminated permissible obtainments from the obtainments here complained of.

144. The odd patterns of these obtainments further demonstrate that they were not made for a permissible purpose.

145. For instance, as shown on Exhibits A and B, there were many instances where personnel from the Defendant Entities looked up the Richard on the same day as his wife, Katherine (Richard listed as "R" and Katherine listed as "K"):

Brooklyn Park	December 20, 2004, 4:22 p.m. (R); 6:06 p.m. (K)
Brooklyn Park	March 15, 2004, 8:48 p.m. (K); 8:49 p.m. (R)
Brooklyn Park	April 8, 2004, 8:21 p.m. (R); 8:22 p.m. (K)

Brooklyn Park	September 18, 2004, 8:44 p.m. (R & K)
Brooklyn Park	March 4, 2005, 9:15 p.m. (R); 9:16 p.m. (K)
Brooklyn Park	April 19, 2005, 9:34 p.m. (R & K)
Brooklyn Park	August 4, 2005, 9:05 p.m. (R & K)
Washington County	September 22, 2005, 11:42 a.m. (K); 11:43 a.m. (R)
Brooklyn Park	March 22, 20106, 9:52 (R & K)
Brooklyn Park	August 8, 2007, 5:12 p.m. (R & K)
Brooklyn Park	February 9, 2008, 9:16 p.m. (R & K)
Hennepin Courts	February 2, 2011, 4:43 p.m. (R & K)

146. Plaintiff and his wife are not criminals. There was no reason permitted under the DPPA for law enforcement to look up both of their Private Data on 12 different occasions – 10 times by law enforcement personnel from Brooklyn Park. The simultaneous accesses of both Richard and Katherine makes clear that Defendant Individuals were interested in them for personal reasons, not related to law-enforcement or other government-related business.

147. Plaintiff was looked up numerous times between the odd hours of 11:00 p.m. to 6:00 a.m.; further indication of the impermissibility of those obtainments.

148. On October 17, 2007, someone from the Pipestone County Sheriffs' Office looked up Richard at 12:05 a.m.

149. On December 28, 2007, someone from the Washington County Sheriff's Office looked up Katherine at 5:01 a.m. and Richard at 5:02 a.m.

150. On April 9, 2008, someone from the Brooklyn Park Police Department looked up both Katherine and Richard at 12:06 a.m.

151. On September 7, 2008, someone from the Brooklyn Park Police Department looked up Richard at 12:26 a.m. and both Richard and Katherine at 12:27 a.m.

152. On September 23, 2008, someone from the Burnsville Police Department looked up Richard at 11:10 p.m.

153. The excess of lookups between these hours suggests that the reason was out of curiosity, animosity, or other reasons not permitted under the DPPA.

154. While law enforcement may work around the clock, law-enforcement investigators typically do not. Rather, investigators generally work day shifts.

155. In the Rasmusson v. City of Bloomington, No. 12-CV-00632 (SRN/JSM) matter, Pine County Sheriff Robin Coles testified that the investigators on his staff typically work day shifts. He further testified that he worked for the Minneapolis Police Department for over 20 years. While he was on the Minneapolis police force, its investigators worked day shifts. See Excerpts of the May 21, 2014 Deposition of Robin K. Cole ("Cole Dep."), attached to the Complaint as Exhibit F at p. 7-8, 18, 41.

156. Thus, late-night DVS look ups of an individual's Private Data, including Plaintiff's Private Data, are likely not being conducted by investigators, investigating a crime. Rather, such look ups are made by patrol officers.

157. Plaintiff's elimination of law-enforcement-related reasons for patrol officers to look them up (not stopped by officers, not being charged with a crime, not

seeking assistance from the police), makes clear that the night time accesses of them private data were made for personal reasons not permitted under the DPPA.

158. Under the direction of the Commissioner Defendants, DPS, and DPS Does, knowingly created the DVS Database that includes Plaintiff's Private Data and the system for law-enforcement personnel to obtain that Data.

159. DPS and DPS Does, under the direction of the Commissioner Defendants, knowingly maintained and updated the DVS and BCA Databases that included Plaintiff's Private Data.

160. DPS Commissioners and DPS Does authored the Minnesota Driver's License Application, which states, "your personal information may be disclosed as authorized by United States Code, title 18, section 2721." (emphasis added).

161. DPS Commissioners and DPS Does made the decisions for establishing, ordering the structure of, and determining the persons, agencies and individuals to whom they would disclose the databases.

162. The disclosure of information was made by providing a user account and a password without reasonably requiring or ensuring that accesses would be limited to those for a purpose permitted under the DPPA.

163. This form of disclosure was and is used not only for law-enforcement personnel but other recipients who have access to the databases, including non-government employees, who comprise about half of the persons who have been granted access to this databases.

164. DPS Does and Commissioner Defendants failed to use reasonable care in so disclosing the information in the databases.

165. DPS Does and Commissioner Defendants made no reasonable effort nor directed any subordinate to make any reasonable effort to require that the specified purpose of the disclosure was legitimate and would be adhered to by the person to whom the data was disclosed.

166. DPS Does and Commissioner Defendants failed to reasonably ascertain or ensure that the persons to whom it was disclosed would use it permissibly.

167. DPS Does and Commissioner Defendants had at the least constructive knowledge of the widespread abuse of the database by officers illegally accessing it for personal reasons not permitted by the DPPA, and had they not delegated their duties to others would have known of the actual misuse and would have presumably fulfilled their statutory duties and prevented the illegal obtainments including those that have adversely affected Plaintiff.

168. DPS Does and Commissioner Defendants knowingly disclosed Plaintiff's data without requiring that the concomitant obtainment was for a permissible purpose; they disclosed it without taking any effective steps to insure adherence by the individuals—whether private or public sector—obtaining it were or would do so for a permissible purpose.

169. DPS Does and Commissioners had no measures in place to prevent or even flag when one individual or different individuals at a municipality obtained the Private

Data of people from the same family or with the same surname within minutes of each other and/or at odd hours. As shown below, other states have such protections.

170. Knowledge of the illegal obtainments of Plaintiff's information by numerous individuals should be imputed to the DPS Does and Commissioner Defendants based in part on their delegation to others of their duty to disclose Private Data for only permissible purposes.

171. DPS Does and Commissioner Defendants failed to ascertain or ensure specifically that law-enforcement personnel would use it permissibly, that is, for a law enforcement function.

172. DPS Does and Commissioner Defendants failed to ascertain or ensure that the persons to whom it was disclosed would use it exclusively for a law-enforcement function.

173. DPS Does and Commissioner Defendants failed to provide adequate training in the permissible uses of the databases.

174. DPS Does and Commissioner Defendants, under 18 U.S.C. § 2724(a), knowingly disclosed Plaintiff's personal information for a purpose not permitted by the DPPA.

175. DPS Does and Commissioner Defendants gave Individual Defendants access to the database for purposes of their intended misuse of the databases.

176. Disclosure of these databases is a matter known to and participated in and directed by the DPS Does and Commissioner Defendants.

177. The DPS Does and Commissioner Defendants had a duty to ascertain the recipients' purpose for his/her obtainment or use of the private data.

178. The DPS Does and Commissioner Defendants, at times, delegated the duty to ascertain the recipients' purpose to other individuals.

179. To the extent the DPS Does and Commissioner Defendants delegated any part of their duties, they are still responsible for disclosure, and the persons, to whom they may have delegated, if any, are not known to Plaintiff and cannot be known by Plaintiff.

180. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2003.

181. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2004.

182. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2005.

183. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2006.

184. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2007.

185. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2008.

186. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2009.

187. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2010.

188. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2011.

189. DPS Does and Commissioner Defendants failed to monitor the databases through regular, random, target, or user audits to assure themselves that the ongoing disclosures were for permissible purposes in 2012.

190. DPS and DPS Does, under the direction of the Commissioner Defendants, had the ability to prevent unauthorized obtainments to the DVS and BCA Databases, including unauthorized obtainment of Plaintiff's Private Data.

191. DPS and DPS Does, under the direction of the Commissioner Defendants, failed to prevent unauthorized access to the DVS and BCA Databases, including access to Plaintiff's Private Data.

192. The Commissioner Defendants and DPS Does knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in the disclosure of Plaintiff's Private Data.

193. The policy of the State of Minnesota is to uphold the provisions of the law, both state and federal, and to protect and safeguard the privacy rights of the State's citizens and inhabitants, including its drivers' privacy rights, and including those rights as are required to be protected by federal law.

194. In particular, it is the policy of the State of Minnesota, as outlined in Minn. Stat. § 171.12, subd. 7, to comply with the provisions and requirements of the DPPA.

195. This policy is also set forth in the driver's license application and set forth in statutory language with proper citation to that federal statute.

196. Defendant Commissioners and DPS Does knowingly disclosed Plaintiff's and others' Private Data and violated state policy by devising and implementing a database, such as the DVS and BCA Databases, that failed abysmally to uphold the privacy rights of Plaintiff and others similarly situated as protected by the DPPA.

197. This failure exposed Plaintiff's information to illegal and knowing obtainments by various persons, including the Defendants in this lawsuit.

198. These acts and failures to act by Defendant Commissioners and DPS Does constitute knowing disclosures of Plaintiff's information within the meaning of the DPPA.

199. Defendant Commissioners and DPS Does knowingly devised and implemented a database and a method for using and misusing that database that both permitted and encouraged, through the nature and monitoring of the system, accesses by law-enforcement personnel, state employees, and others that failed to comply with state policy of protecting privacy rights and complying with the DPPA.

200. The system knowingly devised and implemented by Commissioner Defendants and DPS Does failed to set rules protecting Plaintiff's privacy rights.

201. This system permitted, and on information and belief still permits, the accessing of the database from personal computers.

202. This system allowed individuals to give out their personal passwords to others.

203. This system permitted, and on information and belief may still permit, the accessing of the system by persons without any accountability or even in some instances without the ability to trace the person who made the access.

204. The system allows anyone access to the database when other users fail to log off after their use is completed.

205. From 2003 through 2010, this system did not require reasonably adequate training on the use of the DVS and BCA databases of sworn-law enforcement officers.

206. From 2011 through today, this system still does not require reasonably adequate training on the use of the DVS and BCA databases of sworn law-enforcement officers.

207. Accordingly, the effective monitoring of the system is difficult if not impossible under the system as devised and implemented by Commissioner Defendants and DPS Does.

208. Commissioner Defendants and DPS Does have deliberately emphasized and favored the convenience of the system by users at the expense of protecting the privacy rights of the persons whose information is in the database.

209. This deliberate emphasis and preference for convenience to the system users over the privacy rights of the drivers was known to the Commissioner Defendants and the DPS Does, and was purposeful.

210. In failing to properly implement, maintain, and monitor the DVS and BCA Databases, Commissioner Defendants failed to follow Minnesota state policy.

211. Many viable methods were and are available to prevent this illegal accessing of private information.

212. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were accessing the databases for purposes not permitted under the DPPA.

213. Upon information and belief, the Commissioners and DPS Does actually knew that law-enforcement officers were viewing Plaintiff's Private Data without a legitimate and permissible purpose.

214. Upon information and belief, the Commissioners and DPS Does acquiesced, facilitated, approved, or simply ignored the improper conduct by governmental personnel.

215. Even if the Commissioners and DPS Does had no actual knowledge of the impermissible uses of the databases they oversaw, upon information and belief, they were reckless in their supervision of their subordinates who did operate the databases.

216. Upon information and belief, the Commissioners and DPS Does were negligent in supervising their subordinates who operated the databases.

217. The information contained in the DPS database is far greater and contains more private personal information than is customarily known to non-law enforcement personnel.

218. The information contained in the DPS database includes the social security numbers of the drivers, including Plaintiff's social security number.

219. The information contained in the DPS database includes drivers' health information.

220. These obtainments are committed surreptitiously, and without the knowledge of the victims, including Plaintiff, which knowledge is kept hidden and concealed from the victims, including Plaintiff.

221. There has not been a single instance of which Plaintiff is aware involving his or anyone else where an officer has informed them that he or she has obtained his information.

222. Law-enforcement officers have gone to great lengths to avoid letting Plaintiff know they have obtained his personal private information.

223. The surreptitious, concealed, and hidden obtainments are kept secret from the general public and from the victims, including Plaintiff.

224. Commissioner Defendants and DPS Does allowed multiple breaches of the security of Plaintiff's Private Data in violation of Minn. Stat. 13.055.

225. Commissioner Defendants and DPS Does failed to disclose to Plaintiff this breach of the security of the data in violation of Minn. Stat. 13.055.

226. Obtaining information from the DVS Database without a permissible reason is a breach of confidentiality.

227. Plaintiff contacted DPS to inquire whether law-enforcement officers had been viewing his private information.

228. The DPS website states that the public is entitled to information except that which is classified:

> [T]he law states that all the data DPS or a governmental entity has are public (can be seen by anybody) unless there is a state or federal law that classified the data as not public. You have the right to look at all public data that DPS keeps.

(See "Minnesota Department of Public Safety: Public Access to Government Data," attached to this Complaint as Exhibit C)

229. The DPS website also informs the public that anyone can request information in any way, by phone, in person, mail, or email; that specific data can be requested, or "entire records, files or data bases" or all public data that DPS keeps." It

instructs the person requesting the information that "you don't have to tell us who you are or explain why you are asking for the data." *Id.*

230. But despite its stated policy, before August 2011, the actual practice of DPS was to withhold, deny and mislead the public to prevent access to this information. (See Affidavit of Dan Prozinski, attached to this Complaint as Exhibit D; August 23, 2011 email from Joseph Newton to A. Geraghty, attached to this Complaint as Exhibit E; and the Second Amended Complaint to Kampschroer v. Anoka Cty., et. al, 13-2512 SRN/TNL, at ¶¶ 410 – 426).

231. DPS practice in this regard amounted to concealment of the illegality, by misleading the public on those occasions when they became suspicions about the invasion of their private data.

232. These invasions or illegal obtainments of his Private Data were by their very nature actively concealed, since those making the obtainments concealed them from their supervisors and from Plaintiff; at no time did anyone approach Plaintiff and advise him that he or she had obtained their Private Data.

233. In 2013, Plaintiff requested an audit from Kim Jacobson at DPS.

234. The Minnesota Department of Motor Vehicles is a division of DPS.

235. On April 4, 2013, Jacobson provided the results of the audit to Richard.

236. The audit request and the results furnished were for name look-ups only and specifically did not include any license plate or driver's license number look-ups.

237. Richard was similarly shocked to learn from DPS that it had determined that officers and personnel from approximately several different departments and

agencies had reviewed, and impermissibly obtained or used, his Private Data nearly 50 times since 2003. See Exhibit B.

238. Richard was surprised at the number of agencies on his audit where people had accessed his Private Data, including places where he had never been.

239. Before receiving the DNR letter and requesting the audit reports, Plaintiff had no knowledge that his Private Data had been obtained through the DVS Database.

240. Plaintiff was not under any criminal investigation; he had committed no crimes; he was not seeking the assistance of law-enforcement; he were not a witness to any crime in the Defendant Entities' jurisdictions, nor he involved with anyone in a criminal investigation other than in his duty as a law-enforcement officer, or even a civil lawsuit; he was not of any legitimate interest to law-enforcement other than for personal reasons, such as curiosity or animosity.

241. Richard has not been stopped for a traffic violation since the early to mid-2000s, when he was stopped by the State Patrol for speeding and was given a warning.

242. Before filing suit, Plaintiff (through his attorneys) contacted the Entity Defendants, providing the relevant portion of the audits, sending them a letter in which they requested the Entity to provide them with any permissible reason it or its employees, agents, and officers had in looking up their information; Defendants never provided any legitimate permissible reason for these illegal obtainments.

243. There is no possible law-enforcement function that would have made invading Plaintiff's privacy permissible under the DPPA.

244. Plaintiff believes that even more unauthorized obtainments and viewings will occur in the future if the policies of Entity Defendants and other police departments and law-enforcement agencies similarly situated are not changed to bring the actual custom and practice of these Entity Defendants and others similarly situated into compliance with their own written rules, with the rules of the Department of Public Safety, and with federal law, including the DPPA.

245. Included in the audits are the listing of various law-enforcement departments associated with the Defendant Entities that obtained Plaintiff's Private Data.

246. Individual Defendants' identities (John and Jane Does) are not presently known, and purportedly cannot be revealed pursuant to the Minnesota Government Data Practices Act. Plaintiff anticipates that these yet-to-be-named Individual Defendants will become known through discovery.

247. Supervisor Defendants are not presently known. Plaintiff anticipates that the yet-to-be-named Supervisor Defendants who should have monitored, prevented and stopped the unauthorized accesses to Plaintiff's information will become known through discovery.

248. The remaining Entity Defendant identities (Entity Does) are not presently known, because not all of the entities identified by the DPS have provided sufficient information to determine if their personnel's obtainment of the databases was unauthorized. Plaintiff anticipates that these yet-to-be-named Entity Defendants will become known through discovery.

249. At no time did Plaintiff behave in a manner that would provide any legal justification for the above-described invasion of their privacy.

250. Individual Defendants used the Entity Defendants' computers, passwords and passcodes to obtain Plaintiff's Private Data.

251. The DPPA protects and codifies an individual right to privacy in a person's Private Data, thereby prohibiting unauthorized accessing of all persons' information, including Plaintiff's information.

252. Each individual law-enforcement and other government personnel, acting under color of state and federal law, knew that his or her actions violated and deprived Plaintiff of his clearly established statutory rights under the DPPA.

253. Each Individual Defendant deprived Plaintiff of his federal statutory rights maliciously or by acting with reckless disregard for whether Plaintiff's rights would be violated by his or her actions.

254. Each Individual Defendant was deliberately indifferent to Plaintiff's statutory and civil right to be free from illegal searches, invasions of privacy and the unauthorized accessing of their Private Data.

255. Individual Defendants' numerous accesses of Plaintiff's private information are not unique, but one example of how frequently such law-enforcement agencies and other governmental entities customarily violate the DPPA by accessing Private Data of persons without having any legitimate or permissible reason for doing so.

256. Improper access of citizens' Private Data by Defendants for their own personal and private uses, obtained by accessing that information through the

computerized information storage system kept by the State for official purposes only, is an official custom or practice well known to Defendant Supervisors and Commissioner Defendants.

257. These customs and practices by Defendant Individuals are at variance with the written rules set down by the Entity Defendants, the DPS, and Commissioner Defendants, but these formal rules are widely and knowingly disregarded.

258. Given Entity Defendants' failure to monitor and enforce their rules, the aforementioned customs and practices are attributable to the municipalities themselves, including the Entity Defendants herein.

259. Defendant Entities and Defendant Supervisors of the law-enforcement personnel and other public employees accessing this information knew or should have known of this and other unlawful, improper, unjustified, and impermissible access to private information by law-enforcement personnel and other public employees.

260. The prevalence of this custom, the lack of monitoring regarding these access practices and the failure to take action to stop or prevent these practices, demonstrate the state of mind of Defendant Supervisors and municipal officials of the Entity Defendants.

261. These customs and practices further demonstrate Defendants' deliberate indifference to the federal statutory rights of the citizens and persons, including Plaintiff, whose information has been wrongfully accessed.

262. Defendant Entities are directly liable for the custom and practice of the widespread illegal access of citizens' Private Data.

263. Supervisor Defendants, up to and including the chief police officers and sheriffs employed by each Entity Defendant, are liable in their individual capacity.

264. Defendants' liability is due to their actual and constructive knowledge of this practice.

265. Defendants' liability is also due to their failure to institute any process for monitoring and preventing it.

266. Defendants' liability is also due to their deliberate indifference to the federal rights of those persons, including Plaintiff, whose information has been and continues to be wrongfully accessed.

267. In addition, Defendant Supervisors of the law-enforcement personnel and other public employees, up to and including the chief police officer in each of Defendant Entities, are liable in their individual capacities for the failure to train, monitor, supervise, and properly discipline the officers who are improperly and unlawfully accessing the Private Data of citizens, including Plaintiff, without a proper, lawful, permissible, justifiable purpose for doing so.

268. This pattern of failure to train, monitor, supervise, and discipline demonstrates the state of mind of these Defendant Supervisors and a deliberate indifference to the rights of the citizens and others whose information has been so widely accessed, including Plaintiff.

269. The federal rights of the citizens, including Plaintiff, whose information was improperly accessed, are held in light regard by many if not most of the Defendant Supervisors and by the Defendant Entities themselves.

270. Defendants' lack of concern evidences their deliberate indifference both to the problem of the unauthorized access and to the impact of the unauthorized access on the federal rights of the citizens, including Plaintiff, who would often be unaware of that access.

271. It is yet unknown whether a system has been established by the Entity Defendants and Supervisor Defendants to monitor the regular access of the DPS Databases by personnel.

272. It is yet unknown whether any attempt has been made by Entity Defendants and Supervisor Defendants to provide redress and assurance to the persons, including Plaintiff, whose DVS information has been wrongfully accessed by the Individual Defendants named in this Complaint, or by other personnel in the municipalities named in this Complaint.

273. Defendant Commissioners released and disclosed this information without training or with wholly inadequate training for the individuals with access to the DVS Database.

274. Defendant Commissioners released and disclosed Plaintiff's Private Data to individuals without ascertaining whether it was obtained for a purpose permitted under the DPPA, but instead relied on the status of the person obtaining it, assuming that because of the person's status their obtainment of the information was for a purpose permitted by the DPPA.

275. Whatever training, monitoring, or inquiry into the officers' usage of the information systems has been adopted is woefully inadequate to ensure that access is used properly and lawfully.

276. On information and belief, despite this training, Defendant Entities and Defendant Supervisors, allowed their employees, including but not limited to Individual Defendants, to view Plaintiff's Private Data for unlawful purposes.

277. On information and belief, Defendant Entities, Defendant Supervisors, and Commissioner Defendants permitted, condoned, or acquiesced in this illegal obtainment of Plaintiff's private information, and knew or should have known that it was occurring.

278. On information and belief, this illegal obtainment occurs with regularity not only of Plaintiff's private information, but of other Minnesota drivers' private information.

279. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does have lax policies or lax enforcement of these policies that allow for these intrusions.

280. Defendant Entities, Defendant Supervisors, Defendant Commissioners and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal obtainment of individuals' private information by their officers.

281. As DPS Commissioners, Campion and Dohman, along with DPS Does, were and are responsible for creating, maintaining, and providing access to the database that included Plaintiff's Private Data.

282. Defendant Commissioners and DPS Does also had the ability to determine if unauthorized access was being made and to prevent such unauthorized access to the database, including of Plaintiff's Private Data, and have the ongoing duty to prevent such unauthorized accesses.

283. Defendant Commissioners and DPS Does failed to utilize any due care to ensure that the disclosed information was being used only for permissible purposes.

284. Commissioner Defendants and DPS Does failed to prevent unauthorized access to the database, including Plaintiff's Private Data.

285. On information and belief, Commissioner Defendants, and DPS Does created or oversaw the creation and maintenance of a database and system that was supposed to prevent unauthorized access to Private Data.

286. From 2003, Commissioner Defendants and DPS Does allowed unauthorized access of Plaintiff's Private Data nearly 50 times.

287. On information and belief, Commissioner Defendants' and DPS Does' efforts have been insufficient to prevent future unauthorized access of Plaintiff's and other individuals' private, personal information.

288. Commissioner Defendants and DPS Does have sanctioned the violations by the Individual Defendants through their failure to remedy the policy, custom and practice of officers' and employees' unfettered and unauthorized access to the database.

289. Commissioner Defendants and DPS Does have been negligent in supervising subordinates responsible for implementing a law-enforcement database that prevents unauthorized access to private, personal information.

290. On information and belief, Commissioner Defendants and DPS Does failed to monitor and prevent unauthorized access to private, personal information even though they knew or should have known that such illegal acts were occurring.

291. Commissioner Defendants and DPS Does, acting under the color of state law, were deliberately indifferent to Plaintiff's federal statutory rights to be free from illegal searches, invasions of privacy and the unauthorized accessing of their Private Data.

292. Commissioner Defendants and DPS Does failed to implement properly Minnesota's policy to protect the private, personal information of its citizens with drivers' licenses.

293. Commissioner Defendants and DPS Does are jointly liable for the use, disclosure, or access of Plaintiff's Private Data for each Individual Defendants' access.

294. The Driver's License application assures Minnesota drivers their information will be safeguarded and kept private, "DPS releases this information to local, state, and federal government agencies only as authorized or required by state and federal law."

295. Plaintiff submitted his Private Data to DPS, including his social security number, because of the promise of confidentiality made by DPS.

296. Plaintiff relied on this promise of confidentiality when they provided their Private Data to DPS to obtain a driver's license.

297. The failure of Defendant Entities and Defendant Supervisors to keep this information private is a flagrant breach of a promise of confidentiality.

298. Defendant Entities, Defendant Supervisors, Commissioner Defendants, and DPS Does either have no viable method of or have an inadequate method of ascertaining and controlling the illegal obtainments of individuals' private information by their officers.

299. The extent of this illegal obtaining is widespread and pervasive throughout departments, and is a custom and practice.

300. The widespread practice is demonstrated by the systematic tolerance of illegal obtaining.

301. Each individual with access to the DPS Database has a password allowing that individual access to the DPS Database.

302. Personnel can access the DPS Databases from any computer with Internet access.

303. Personnel occasionally gave other individuals their passwords, contrary to requirements.

304. The system for accessing accountability and responsibility was and is prone to error and fails to reasonably protect drivers' private information.

305. When Defendant personnel viewed Plaintiff's private information, they did not do so to carry out official police functions.

306. Plaintiff committed no crimes or transgressions that would explain or legitimize the unauthorized obtainment of his Private Data.

307. The Individual Defendants obtained Plaintiff's personal information without probable cause or reasonable suspicion to believe that Plaintiff had engaged in any criminal activity or any activity even remotely related to criminal activity.

308. Plaintiff never waived the protections of the DPPA.

309. Defendants' actions have violated the DPPA.

310. The sheer volume of the intrusions into his private life, the odd hours of the accesses, the pattern of both Richard and Katherine having their information obtained within minutes of each other, the admission by Brooklyn Park that Rivard was looking up Richard and Katherine, and the Plaintiff's lack of official contact with the Defendant Entities demonstrates that law-enforcement personnel, public employees, and others are unfairly hostile and careless toward Plaintiff's privacy and safety.

311. As a result of these invasions of privacy, Plaintiff has suffered and continues to suffer emotional distress.

THE COMMISSIONERS HAVE KNOWN ABOUT THESE VIOLATIONS

312. DPS Commissioners Campion and Dohman have been involved with law enforcement for many years.

313. Commissioner Dohman has been a law enforcement officer for thirty years, having formerly served as police chief of the City of Maple Grove from 2001 until her appointment as DPS Commissioner in March 2011.

314. Before becoming Chief of Police of the Maple Grove Police Department she was an investigator, patrol officer, sergeant and captain of the Maple Grove Police

Department; and prior to that time, she was a patrol officer of the City of Glencoe and of the City of Marshall, Minnesota.

315. Dohman also served as president of the Minnesota Chiefs of Police Association.

316. Upon information and belief, the misuse of private information is the main complaint of most police chiefs and human resources personnel.

317. Former Commissioner Michael Campion served from July 2004 until March 2011. Prior to his appointment as DPS Commissioner he was supervisor of the BCA, which also maintains a driver's license database.

318. Prior to that position, Campion was a special agent at the BCA.

319. It was during his tenure that the DPS database was largely developed in its current format.

320. On information and belief, misuse of the DPS database has been well-known to Commissioner Defendants. At a Legislative Audit Subcommittee hearing in February, 2013 at which Commissioner Dohman testified, the testimony of the Legislative Auditor revealed that at least 50% of law enforcement officers are misusing the DPS database by obtaining, disclosing, and/or using the driver license personal information for an impermissible purpose.

321. On information and belief, Commissioner Defendants knew this, and knowingly disclosed the information in part by (a) failing to safeguard and monitor the database despite knowing of its rampant misuse, (b) willfully refusing to correct the

misuses, or (c) both failing to monitor and refusing to correct the abuse and misuse of the system.

322. Experts in the field of police training report that the primary complaint of many police departments is that law-enforcement personnel misuse private information. This is an established, well-known, and pervasive problem with law enforcement that Commissioner Defendants are unwilling to properly address.

323. Dohman admitted that she is responsible for the breach of the database.

324. In an article published in the April/May 2013 issue of the Minnesota Police Journal, Dohman, writing as Commissioner of the Public Safety, wrote, "We can all agree that no one should be above the law; we are all accountable for our action. Those of use entrusted with protecting the public, along with its rights, are especially accountable, in my view." (See Exhibit B, Mona Dohman, Commissioner of Public Safety, "Protecting Minnesota's DVS Database with Training, Oversight and Integrity," Minnesota Police Journal, April/May 2013).

THE COMMISSIONER DEFENDANTS AND DPS DOES REASONABLY COULD HAVE DONE SIGNIFICANTLY MORE TO PROTECT PLAINTIFF'S PRIVACY.

325. On information and belief, the only changes and improvements to the DPS system to increase the protection of privacy, especially from law enforcement, have occurred only after litigation involving DPS, specifically the lawsuit titled Anne Marie Rasmusson v. City of Bloomington, No. 12-CV-00632 (SRN/JSM). In that case Plaintiff sued, among others, the Commissioners of the DPS and was able to obtain through settlement significant changed to the DVS database, including numerous protections such

as different types of periodic audits. On information and belief, the 19,000 improper accesses of former Department of Natural Resources Captain John Hunt were discovered in part due to those changes. The vast majority of the restrictions and protections on driver privacy have occurred due to the Rasmusson case and others like it. The Commissioners in Minnesota remain highly resistant to improving the DPS database, instead looking to the individual officers and local governments to institute changes, which is a far less effective method of instituting changes and will result in piecemeal and inadequate changes in protections at best.

326. On information and belief, states other than Minnesota have far greater restrictions and protections in place to protect the data on their drivers' license databases from being obtained, disclosed or used for a reason not permitted by the DPPA.

327. For instance, on further information and belief, North Dakota requires a daily report of anyone who obtains driver photos and its system generates weekly reports listing all individuals with accesses of over 25 images a day. These reports are sent to the North Dakota Attorney General to make inquiries as to whether the information was obtained for a job-related reason. North Dakota also requires the users of the database to declare the reason why they were looking at the record. North Dakota also requires its users to take a certification test before being given access to the database.

328. Also on information and belief, the State of California's DMV cooperates with its law-enforcement agencies and California's Department of Justice to ensure access to its drivers' license information is limited to agencies that satisfy specific requirements before they are issued a confidential requester code that permits access to

law-enforcement information only. Each law-enforcement agency is responsible for limiting access to necessary personnel. California also periodically reviews law-enforcement applications to ensure the agency and person requesting the information is still entitled to obtain the information. During a recent audit, California's DMV reviewed questionable agencies and even reclassified some to prevent them from having further access to the database.

329. On further information and belief, the California DMV has a dedicated law-enforcement unit to analyze data inquiries. Each data request is logged and technicians are trained to look for developing patterns in the requester's history. The California DMV also conducts periodic historical reviews of a specific agency's requests to determine if the accesses were authorized. The California DMV may also require a law-enforcement entity to supply an explanation of events, describe their protocols for accessing DMV information, what policies or access requirements were violated, what corrective or administrative steps are being taken to admonish the officer, and what steps the agency is taking to avoid future occurrences. All users annually complete an information security form. Finally, the California DMV is very restrictive on the types of information it releases.

330. In addition, private businesses have protections in place to prevent misuse of Private Data. For instance, Thompson Reuters, when conducting a Public Records search on its "Westlaw Next" platform, it warns users that "Use of this data is limited by the Driver's Privacy Protection Act (DPPA) and state law." Thompson-Reuters then has a drop down box that drops down asking the user to, "Please acknowledge your

permissible use under the Driver's Privacy Protection Act," and select the permissible purpose under the DPPA that they have for obtaining the Private Data. (See Exhibit G, which is a screen shot from the Westlaw Next Personal Records page).

331. On information and belief, DPS Commissioners, DPS and Defendants Entities knew or should have known of the policies and practices of other States and private businesses, but did not at the time that Plaintiff's drivers' license information was being impermissibly obtained, require any of the protections and safeguards to the Minnesota DPS Databases utilized by other states.

332. Given that other states and private businesses do and did have safeguards and protections in place to protect their drivers' private information from impermissible obtaining, use, and disclosure, DPS Commissioners, DPS and Defendants Entities reasonably should have implemented such safeguards and protections for Minnesota drivers, including Plaintiff.

333. The implementation of some or all of these safeguards and protections by Defendants would have prevented many of the impermissible obtainment, uses, and disclosures of Plaintiff's private data.

COUNT I: VIOLATION OF THE DPPA, 18 U.S.C. § 2721, *et seq.*

(Against all Defendants)

334. Plaintiff reaffirms and realleges the allegations in Paragraphs 1 through 333.

335. Plaintiff provided personal information to the DPS including his address, color photographs, date of birth, weight, height, eye color, and social security number for

the purpose of acquiring and utilizing a State of Minnesota driver's license. The DPS Database also maintained Plaintiff's driving record.

336. Plaintiff did not provide his consent for any of Defendant Individuals to obtain, disclose or use, or for any of Defendant Entities or Defendant Supervisors to disclose or to allow Defendant Individuals to obtain, disclose or use his private information for anything but official law-enforcement business.

337. Knowingly obtaining, disclosing or using Private Data for a purpose not permitted by the DPPA is a violation of the DPPA. The statute provides for criminal fines and civil penalties. 18 U.S.C. §§ 2723, 2724.

338. The DPPA provides redress for violations of a person's protected interest in the privacy of their motor vehicle records and the identifying information therein.

339. Minnesota law is to enforce and follow the DPPA and to hold all information obtained pursuant to an application for a driver's license confidential and private; even prior to the passage of the DPPA in 1994 Minnesota law pledged to hold all this information private and confidential, and on one's driver's license application these promises of confidentiality are all made; Defendants' actions in accessing this information is a flagrant breach of that pledge of confidentiality.

340. Each of the Defendants invaded Plaintiff's legally protected interest under the DPPA.

341. According to the Department of Vehicle Services, the Individual Defendants knowingly obtained, disclosed or used Plaintiff's personal information, from

a motor vehicle record, for a purpose not permitted under the DPPA. 18 U.S.C. § 2724(a).

342. None of the Individual Defendants' activities fell within the DPPA's permitted exceptions for procurement of Plaintiff's private information.

343. By the actions described above, each Defendant Individual was acting within the scope of his or her employment when he or she obtained, disclosed or used Plaintiff's personal information from the DPS Databases for a purpose not permitted by the DPPA.

344. Individual Defendants knew that their actions related to Plaintiff's Private Data were in violation of the DPPA.

345. Defendant Entities and Defendant Supervisors knowingly authorized, directed, ratified, approved, acquiesced in, committed or participated in obtaining, disclosing or using of Plaintiff's private personal information by Individual Defendants.

346. Defendant Commissioners, Defendant Entities and Defendant Supervisors' actions constitute a knowing disclosure of the personal information of Plaintiff under the DPPA.

347. Individual Defendants knowingly used Defendant Entities' computers, passwords and passcodes to obtain Plaintiff's private information.

348. Plaintiff's private information was obtained by each Individual Defendant for purposes that are not permitted under the DPPA.

349. Defendant Entities are each vicariously liable for the acts of Defendant Individuals.

350. By the actions complained of, Commissioner Defendants, and DPS Does are jointly liable for the acts of Defendant Individuals.

351. Plaintiff has suffered harm because his private information has been obtained and viewed unlawfully.

352. Plaintiff has further suffered harm because his private information has been obtained unlawfully. Plaintiff suffered and continues to suffer harm by virtue of the increased risk that his protected information is in the possession of Individual Defendants who obtained it without a legitimate purpose.

353. This is precisely the harm Congress sought to prevent by enacting the DPPA and its statutory remedies.

354. Individual Defendants, Supervisor Defendants, and Commissioner Defendants each willfully and recklessly disregarded the law, entitling Plaintiff to punitive damages under the DPPA, see 18 U.S.C. § 2724(b)(2), which is not subject to the pleading requirement of Minnesota state law as set forth in Minn. Stat. § 549.20. Plaintiff is entitled to actual damages, punitive damages, reasonable attorneys' fees and other litigation costs reasonably incurred, and such other preliminary and equitable relief as the court determines to be appropriate. 18 U.S.C. § 2724(b).

355. In addition, under the DPPA, Plaintiff is entitled to a baseline liquidated damages award of at least $2,500 for each violation of the DPPA. 18 U.S.C. § 2721(b)(1). Plaintiff need not prove actual damages to receive said liquidated damages.

JURY DEMAND

356. Plaintiff demands a jury trial as to all issues of fact herein properly triable to a jury under any statute or under common law.

WHEREFORE, Richard Sapp prays for judgment against the Defendants as follows:

1. A money judgment against all Defendants for liquidated, actual and compensatory damages in an amount in excess of seventy five thousand ($75,000) dollars and punitive damages in an amount to be determined by the jury, together with their costs, including reasonable attorney fees, under 42 U.S.C. § 1988, the DPPA, and other applicable laws, and prejudgment interest;

2. Actual damages, punitive damages, attorneys' fees and other litigation costs and such other preliminary and equitable relief as the court determines to be appropriate under 18 U.S.C. § 2724(b);

3. Liquidated damages of at least $2,500 for each violation of the DPPA under 18 U.S.C. § 2721(b)(1);

4. An injunction, permanently enjoining all Defendants from viewing Ray's private information in violation of the DPPA, unless necessary for law enforcement purposes;

5. An injunction, permanently and prospectively requiring Defendants to establish and implement all effective monitoring and investigative procedures to end this practice, discover and suspend permanently all accessing privileges to the violators; and

to provide full disclosure to all potential claimants of the entities and persons who have violated their rights under the DPPA and the Constitution; and,

6. For such other and further relief as this Court deems just and equitable.

SAPIENTIA LAW GROUP PLLC

Dated: March 25, 2014

s/Jonathan A. Strauss
Jonathan A. Strauss (#0279602)
Lorenz F. Fett (#196769)
Sonia Miller-Van Oort (#278087)
12 South Sixth Street, Suite 1242
Minneapolis, MN 55402
(612) 756-7100, Fax: 612-756-7101
jons@sapientialaw.com
larryf@sapientialaw.com
soniamv@sapientialaw.com

and

SIEBEN CAREY

s/Susan M. Holden
Susan M. Holden (#0189844)
Jeffrey M. Montpetit (#0291249)
901 Marquette Avenue
Suite 500
Minneapolis, MN 55402
(612) 333-4500
Jeffrey.Montpetit@Knowyourrights.com
Susan.Holden@Knowyourrights.com

ATTORNEY FOR PLAINTIFF RICHARD SAPP